(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020060059853 A
(43)Date of publication of application: 02.06.2006

(21)Application number: 1020057004722
(22)Date of filing: 18.03.2005
(30)Priority: 18.09.2002 JP2002 2002271473

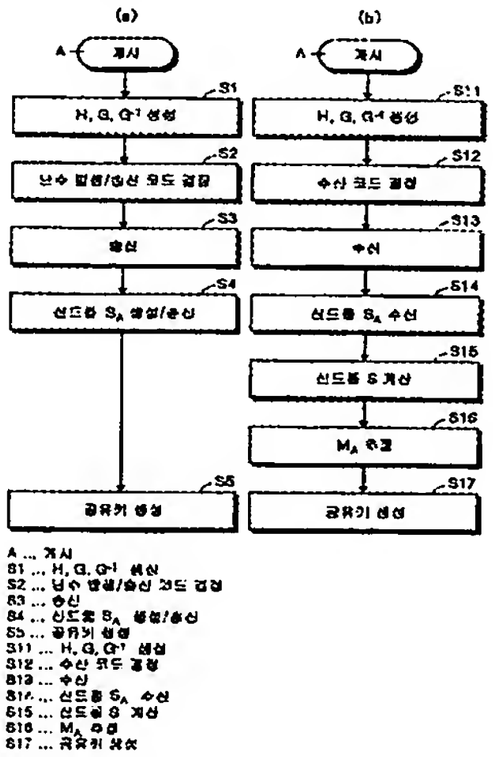
(51)Int. Cl H04L 9/08 H04L 9/28 H03M 13/11 G11B 20/18

(71)Applicant: MITSUBISHI ELECTRIC CORPORATION
(72)Inventor: MATSUMOTO WATARU WATANABE YOUDAI

(54) QUANTUM KEY DISTRIBUTION METHOD AND COMMUNICATION DEVICE

(57) Abstract:

It is possible to create a shared key whose safety is surely guaranteed while correcting a data error in the transmission path by using an error correction code having an extremely high characteristic. According to a quantum key distribution method, firstly, a communication device of the reception side corrects the data error of the reception data by using a parity inspection matrix for an Irregular-LDPC code which is determinate and has stable characteristic. The communication device of the reception side and the communication device of the transmission side discard a part of shared information according to the error correction information disclosed.



Legal Status
Date of request for an examination (20050321)
Notification date of refusal decision ( )
Final disposal of an application (registration)
Date of final disposal of an application (20061226)
Patent registration number (1006974760000)
Date of registration (20070313)
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )

(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.
H04L 9/08 (2006.01)
H04L 9/28 (2006.01)
H03M 13/11 (2006.01)
G11B 20/18 (2006.01)

(11) 공개번호 10-2006-0059853
(43) 공개일자 2006년06월02일

(21) 출원번호 10-2005-7004722
(22) 출원일자 2005년03월18일
번역문 제출일자 2005년03월18일
(86) 국제출원번호 PCT/JP2003/011706
국제출원일자 2003년09월12일
(87) 국제공개번호 WO 2004/028074
국제공개일자 2004년04월01일

(30) 우선권주장 JP-P-2002-00271473 2002년09월18일 일본(JP)

(71) 출원인 미쓰비시덴키 가부시키가이샤
일본국 도쿄도 지요다쿠 마루노우치 2쵸메 7반 3고

(72) 발명자 마츠모토 와타루
일본 도쿄도 지요다쿠 마루노우치 2쵸메 2반 3고 미쓰비시덴키가부시키가이샤 내
와타나베 요다이
일본 사이타마켄 와코시 히로사와 2반 1고 리가가쿠 겐큐쇼 내

(74) 대리인 김창세

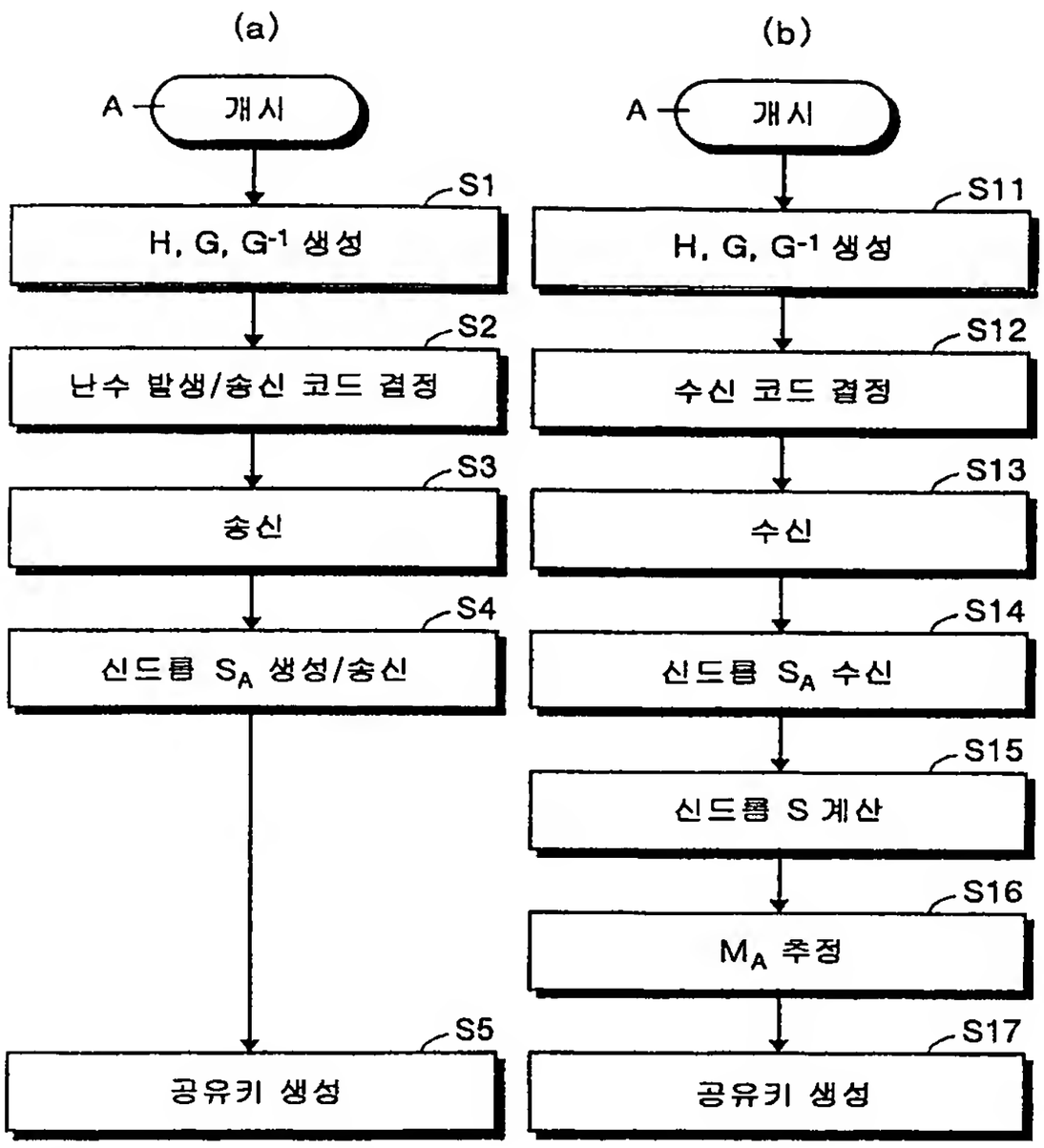
심사청구 : 있음

(54) 양자키 배송 방법 및 통신 장치

요약

극히 높은 특성을 가진 오류 정정 부호를 이용하여 전송로 상에서의 데이터 오류를 정정하면서, 고도로 안전성이 보증된 공통키를 생성하기 위해, 본 발명의 양자키 배송 방법에서는, 우선, 수신측의 통신 장치가, 확정적이고 특성이 안정된 「Irregular-LDPC 부호」용의 패리티 검사 행렬을 이용하여 수신 데이터의 데이터 오류를 정정한다. 그리고, 수신측의 통신 장치 및 송신측의 통신 장치가 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버리는 것으로 했다.

대표도



A ... 개시
S1 ... H, G, G^{-1} 생성
S2 ... 난수 발생/송신 코드 결정
S3 ... 송신
S4 ... 신드롬 S_A 생성/송신
S5 ... 공유키 생성
S11 ... H, G, G^{-1} 생성
S12 ... 수신 코드 결정
S13 ... 수신
S14 ... 신드롬 S_A 수신
S15 ... 신드롬 S 계산
S16 ... M_A 추정
S17 ... 공유키 생성

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야

본 발명은 고도로 안전성이 보증된 공통키를 생성하는 것이 가능한 양자키 배송 방법에 관한 것이며, 특히, 오류 정정 부호를 이용하여 데이터 오류를 정정할 수 있는 양자키 배송 방법 및 당해 양자키 배송을 실현 가능한 통신 장치에 관한 것이다.

종래의 기술

이하, 종래의 양자 암호 시스템에 대하여 설명한다. 최근, 고속 대용량인 통신 기술로서 광통신이 널리 이용되고 있지만, 이러한 광통신 시스템에서는, 광의 온/오프로 통신이 행해지고, 온일 때에 대량의 광자가 송신되고 있기 때문에, 양자 효과가 직접 나타나는 통신계로는 되어 있지 않다.

한편, 양자 암호 시스템에서는, 통신 매체로서 광자를 이용하여, 불확정성 원리 등의 양자 효과가 발생하도록 1개의 광자로 1 비트의 정보를 전송한다. 이 때, 도청자가, 그 편광, 위상 등의 양자 상태를 모르고 적당히 기저를 골라 광자(光子)를 측정하면, 그 양자 상태에 변화가 발생한다. 따라서, 수신측에서는, 이 광자의 양자 상태의 변화를 확인함으로써, 전송 데이터가 도청됐는지 여부를 인식할 수 있다.

도 9는 종래의 편광을 이용한 양자키 배송의 개요를 나타내는 도면이다. 예컨대, 수평수직 방향의 편광을 식별 가능한 측정기에서는, 양자 통신로 상의, 수평 방향(0°)으로 편광된 광과 수직 방향(90°)으로 편광된 광을 정확하게 식별한다. 한편, 경사 방향(45°, 135°)의 편광을 식별 가능한 측정기에서는, 양자 통신로 상의, 45° 방향으로 편광된 광과 135° 방향으로 편광된 광을 정확하게 식별한다.

이와 같이, 각 측정기는, 규정된 방향으로 편광된 광에 대해서는 정확하게 인식할 수 있지만, 예컨대, 경사 방향으로 편광된 광을 수평수직 방향(0°, 90°)의 편광을 식별 가능한 측정기에 의해 측정하면, 수평 방향과 수직 방향으로 편광된 광을 각각 50%의 확률로 랜덤하게 식별한다. 즉, 식별 가능한 편광 방향에 대응하지 않는 측정기를 이용한 경우에는, 그 측정 결과를 해석하더라도, 편광된 방향을 정확하게 식별할 수가 없다.

도 9에 나타내는 종래의 양자키 배송에서는, 상기 불확정성(랜덤성)을 이용하여, 도청자에게 알려지지 않고 송신자와 수신자 사이에서 키를 공유한다(예컨대, 비특허문헌 1 참조). 또, 송신자 및 수신자는, 양자 통신로 이외로 공개 통신로를 사용할 수 있다. 여기서, 키의 공유 수순에 대하여 설명한다.

우선, 송신자는, 난수열(1, 0의 열: 송신 데이터)을 발생시키고, 또한 송신 코드(+ : 수평수직 방향으로 편광된 광을 식별 가능한 측정기에 대응, ×: 경사 방향으로 편광된 광을 식별 가능한 측정기에 대응)를 랜덤하게 결정한다. 그 난수열과 송신 코드의 조합으로, 송신하는 광의 편광 방향이 자동적으로 정해진다. 여기서는, 0과 + 의 조합으로 수평 방향으로 편광된 광을, 1과 + 의 조합으로 수직 방향으로 편광된 광을, 0과 ×의 조합으로 45° 방향으로 편광된 광을, 1과 ×의 조합으로 135° 방향으로 편광된 광을, 양자 통신로에 각각 송신한다(송신 신호).

다음에, 수신자는, 수신 코드(+ :수평수직 방향으로 편광된 광을 식별 가능한 측정기, ×:경사 방향으로 편광된 광을 식별 가능한 측정기)를 랜덤하게 결정하고, 양자 통신로 상의 광을 측정한다(수신 신호). 그리고, 수신 코드와 수신 신호의 조합에 의해 수신 데이터를 얻는다. 여기서는, 수신 데이터로서, 수평 방향으로 편광된 광과 + 의 조합으로 0을, 수직 방향으로 편광된 광과 + 의 조합으로 1을, 45° 방향으로 편광된 광과 ×의 조합으로 0을, 135° 방향으로 편광된 광과 ×의 조합으로 0을, 각각 얻는다.

다음에, 수신자는, 자신의 측정이 정확한 측정기로 행해진 것인지 여부를 조사하기 위해서, 수신 코드를, 공개 통신로를 거쳐서 송신자에 대하여 송신한다. 수신 코드를 수취한 송신자는, 정확한 측정기로 행하여진 것인지 여부를 조사하여, 그 결과를, 공개 통신로를 거쳐서 수신자에 대하여 회신한다.

다음에, 수신자는, 정확한 측정기로 수신한 수신 신호에 대응하는 수신 데이터만을 남기고, 그 이외의 것을 버린다. 이 시점에서, 남겨진 수신 데이터는 송신자와 수신자 사이에서 확실히 공유되어 있다.

다음에, 송신자와 수신자는 각각의 통신 상대에 대하여 공유 데이터 중에서 선택한 소정수의 데이터를, 공개 통신로를 경유하여 송신한다. 그리고, 수취한 데이터가 자신이 가진 데이터와 일치하고 있는지 여부를 확인한다. 예컨대, 확인한 데이터 중에 일치하지 않는 데이터가 하나라도 있으면, 도청자가 있는 것으로 판단하여 공유 데이터를 버리고, 다시, 키의 공유 수순을 처음부터 다시 한다. 한편, 확인한 데이터가 전부 일치한 경우에는, 도청자가 없다고 판단하여, 확인에 사용한 데이터를 버리고, 남은 공유 데이터를 송신자와 수신자의 공유키로 한다.

또한, 상기 종래의 양자키 배송 방법의 응용으로서, 예컨대, 전송로 상에서의 데이터 오류를 정정 가능한 양자키 배송 방법이 있다(예컨대, 비특허문헌 2참조).

이 방법에서는, 송신자가, 데이터 오류를 검출하기 위해서, 송신 데이터를 복수의 블럭으로 분할하고, 블럭마다의 패리티를 공개 통신로 상에 송신한다. 그리고, 수신자가, 공개 통신로를 경유하여 수취한 블럭마다의 패리티와 수신 데이터에 있어서의 대응하는 블럭의 패리티를 비교하여, 데이터 오류를 체크한다. 이 때, 다른 패리티가 있었던 경우, 수신자는, 어떤 블럭의 패리티가 다른 것인지를 나타내는 정보를 공개 통신로 상에 회신한다. 그리고, 송신자는, 해당하는 블럭을 전반부의 블럭과 후반부의 블럭으로 더 분할하고, 예컨대, 전반부의 패리티를 공개 통신로 상에 회신한다(이분 탐색(binary search)). 이후, 송신자와 수신자는 상기 이분 탐색을 반복하여 실행함으로써 오류 비트의 위치를 특정하고, 최종적으로 수신자가 그 비트를 정정한다.

또한, 송신자는, 데이터에 오류가 있음에도 불구하고, 우수개의 오류 때문에 옳다고 판정된 패리티가 있는 경우를 상정하고, 송신 데이터를 랜덤하게 치환하여(랜덤 치환) 복수의 블럭으로 분할하고, 다시, 상기 이분 탐색에 의한 오류 정정 처리를 한다. 그리고, 랜덤 치환에 의한 이 오류 정정 처리를 반복하여 실행함으로써, 모든 데이터 오류를 정정한다.

[비특허문헌 1]

Bennett, C. H. and Brassard, G.:Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC.1984).

[비특허문헌 2]

Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

그러나, 상기 도 9에 나타내는 종래의 양자키 배송에 있어서는, 오류 통신로를 상정하지 않기 때문에, 오류가 있는 경우에는 도청 행위가 존재한 것으로 하여 상기 공통 데이터(공통키)를 버리는 것으로 되고, 전송로에 따라서는 공통키의 생성 효율이 매우 나빠진다는 문제가 있었다.

또한, 상기 전송로 상에서의 데이터 오류를 정정 가능한 양자키 배송 방법에 있어서는, 오류 비트를 특정하기 위해서 방대한 회수의 패리티의 교환이 발생하고, 또한, 랜덤 치환에 의한 오류 정정 처리가 소정 회수에 걸쳐 행하여지기 때문에, 오류 정정 처리에 막대한 시간을 쓰는 것으로 된다는 문제가 있었다.

따라서, 본 발명은, 극히 높은 특성을 가진 오류 정정 부호를 이용하여 전송로 상에서의 데이터 오류를 정정하면서, 고도로 안전성이 보증된 공통키를 생성하는 것이 가능한 양자키 배송 방법을 제공하는 것을 목적으로 하고 있다.

발명의 상세한 설명

본 발명에 따른 양자키 배송 방법에 있어서는, 광자를 양자 통신로 상에 송신하는 제 1 통신 장치와 당해 광자를 측정하는 제 2 통신 장치로 구성된 양자 암호 시스템에 의해 실행되고, 예컨대, 상기 제 1 및 제 2 통신 장치가, 동일한 패리티 검사 행렬 H(n×k)을 생성하는 검사 행렬 생성 단계와, 상기 제 1 통신 장치가, 난수열(송신 데이터)을 발생시키고, 또한 소정의 송신 코드(기저)를 랜덤하게 결정하며, 상기 제 2 통신 장치가 소정의 수신 코드(기저)를 랜덤하게 결정하는 난수 발생 단계와, 상기 제 1 통신 장치가, 상기 송신 데이터와 송신 코드의 조합에 의해 규정된 양자 상태에서, 광자를 양자 통신로 상에 송신하는 광자 송신 단계와, 상기 제 2 통신 장치가, 양자 통신로 상의 광자를 측정하고, 상기 수신 코드와 측정 결과의 조합에 의해 규정된 수신 데이터를 얻는 광자 수신 단계와, 상기 제 1 및 제 2 통신 장치가, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하여, 정확한 측정기로 측정된 n 비트의 수신 데이터 및 대응하는 송신 데이터를 남기고, 그 이외의 것을 버리는 데이터 삭제 단계와, 상기 제 1 통신 장치가, 상기 패리티 검사 행렬 H와 n 비트의 송신 데이터에 근거한 k 비트의 오류 정정 정보를, 공개 통신로를 거쳐서 상기 제 2 통신 장치에 통지하는 오류 정정 정보 통지 단계와, 상기 제 2 통신 장치가, 상기 패리티 검사 행렬 H와 n 비트의 수신 데이터와 오류 정정 정보에 근거하여, 수신 데이터의 오류를 정정하는 오류 정정 단계와, 상기 제 1 및 제 2 통신 장치가, 공개된 오류 정정 정보에 따라 오류 정정 후의 공유 정보(n)의 일부(k)를 버리고, 나머지 정보로 암호키를 생성하며, 이 암호키를 장치간의 공유키로 하는 암호키 생성 단계를 포함하는 것을 특징으로 한다.

본 발명에 의하면, 확정적이고 특성이 안정된 「Irregular-LDPC 부호」용의 패리티 검사 행렬을 이용하여 공유 정보의 데이터 오류를 정정하고, 또한, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버린다.

도면의 간단한 설명

도 1은 본 발명에 따른 양자 암호 시스템의 실시예 1의 구성을 나타내는 도면,

도 2는 실시예 1의 양자키 배송을 나타내는 흐름도,

도 3은 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」의 구성법을 나타내는 흐름도,

도 4는 유한 아핀 기하 부호 AG(2, 2^2)의 매트릭스를 나타내는 도면,

도 5는 최종적인 열의 가중치 배분 $\lambda(\gamma_i)$과 행의 가중치 배분 ρ_u를 나타내는 도면,

도 6은 랜덤 계열의 라틴 방진 행렬(latin square matrix)에 의한 분할 수순을 나타내는 도면,

도 7은 본 발명에 따른 양자 암호 시스템의 실시예 2의 구성을 나타내는 도면,

도 8은 실시예 2의 양자키 배송을 나타내는 흐름도,

도 9는 종래의 양자키 배송의 개요를 나타내는 도면.

실 시 예

이하에, 본 발명에 따른 양자키 배송 방법의 실시예를 도면에 근거하여 상세히 설명한다. 또, 이 실시예에 따라 본 발명이 한정되는 것이 아니다. 또한, 이하에서는, 예로서 편광을 이용하는 양자키 배송에 대하여 설명하지만, 본 발명은, 예컨대, 위상을 이용하는 것, 주파수를 이용하는 것 등에도 적용 가능하고, 어떠한 양자 상태를 이용하는지에 대해서는 특히 한정하지 않는다.

(실시예 1)

양자키 배송은, 도청자의 계산 능력에 상관없이, 안전성이 보증된 키 배송 방식이지만, 예컨대, 보다 효율적으로 공유키를 생성하기 위해서는, 전송로를 지나는 것에 따라 발생하는 데이터의 오류를 제거할 필요가 있다. 그래서, 본 실시예에서는, 극히 높은 특성을 갖는 것이 알려져 있는 저밀도 패리티 검사(LDPC: Low-Density Parity-Check) 부호를 이용하여 오류 정정을 하는 양자키 배송에 대하여 설명한다.

도 1은 본 발명에 따른 양자 암호 시스템에서의 통신 장치(송신기, 수신기)의 구성을 나타내는 도면이다. 이 양자 암호 시스템은, 정보 m_a를 송신하는 기능을 구비한 송신측의 통신 장치와, 전송로 상에서 잡음 등의 영향을 받은 정보 m_a, 즉 정보 m_b를 수신하는 기능을 구비한 수신측의 통신 장치로 구성된다.

또한, 송신측의 통신 장치는, 양자 통신로를 거쳐서 정보 m_a를 송신하고, 공개 통신로를 거쳐서 신드롬 s_A를 송신하며, 이들 송신 정보에 근거하여 암호키(수신측과의 공통키)를 생성하는 암호키 생성부(1)와, 암호화부(21)가 암호키에 근거하여 암호화한 데이터를, 송수신부(22)가 공개 통신로를 거쳐 주고받는 통신부(2)를 구비하고, 수신측의 통신 장치는, 양자 통신로를 거쳐서 정보 m_b를 수신하며, 공개 통신로를 거쳐서 신드롬 s_A를 수신하고, 이들 수신 정보에 근거하여 암호키(송신측과의 공통키)를 생성하는 암호키 생성부(3)와, 암호화부(42)가 암호키에 근거하여 암호화한 데이터를, 송수신부(41)가 공개 통신로를 거쳐 교환하는 통신부(4)를 구비한다.

상기 송신측의 통신 장치에서는, 양자 통신로 상에 송신하는 정보 m_a로서, 편광 필터를 이용하여 소정의 방향으로 편광시킨 광(도 9 참조)을, 수신측의 통신 장치에 대하여 송신한다. 한편, 수신측의 통신 장치에서는, 수평수직 방향(0°, 90°)의 편광을 식별 가능한 측정기와 경사 방향(45°, 135°)의 편광을 식별 가능한 측정기를 이용하여, 양자 통신로 상의, 수평 방향(0°)으로 편광된 광과 수직 방향(90°)으로 편광된 광과 45° 방향으로 편광된 광과 135° 방향으로 편광된 광을 식별한다. 또, 각 측정기는, 규정된 방향으로 편광된 광에 대해서는 정확하게 인식할 수 있지만, 예컨대, 경사 방향으로 편광된 광을 수평수직 방향(0°, 90°)의 편광을 식별 가능한 측정기에 의해 측정하면, 수평 방향과 수직 방향으로 편광된 광을 각각 50%의 확률로 랜덤하게 식별한다. 즉, 식별 가능한 편광 방향에 대응하지 않는 측정기를 이용한 경우에는, 그 측정 결과를 해석하더라도, 편광된 방향을 정확하게 식별할 수가 없다.

이하, 상기 양자 암호 시스템에서의 각 통신 장치의 동작, 즉, 본 실시예에서의 양자키 배송에 대하여 상세히 설명한다. 도 2는 본 실시예의 양자키 배송을 나타내는 흐름도, 상세하게는, (a)는 송신측의 통신 장치의 처리를 나타내고, (b)는 수신측의 통신 장치의 처리를 나타낸다.

우선, 상기 송신측의 통신 장치 및 수신측의 통신 장치에서는, 패리티 검사 행렬 생성부(10, 30)가, 특정 선형 부호의 패리티 검사 행렬 H(n×k)을 구하며, 이 패리티 검사 행렬 H로부터 「HG=0」을 만족시키는 생성 행렬 G((n-k)×n)을 구하고, 또한, G^{-1}·G=I(단위 행렬)로 되는 G의 역행열 G^{-1}(n×(n-k))을 구한다(단계 S1, 단계 S11). 본 실시예에서는, 상기 특정

선형 부호로서, 샤논한계(Shannon limit)에 극히 가까운 우수한 특성을 갖는 LDPC 부호를 이용한 경우의 양자키 배송에 대하여 설명한다. 또, 본 실시예에서는, 오류 정정 방식으로서 LDPC 부호를 이용하는 것으로 했지만, 이것에 한정되지 않고, 예컨대, 터보 부호 등의 다른 선형 부호를 이용하는 것으로 해도 좋다. 또한, 예컨대, 후술하는 오류 정정 정보(신드롬)가 적당한 행렬 H와 정보 m_A의 적 Hm_A로 표시되는 오류 정정 프로토콜(예컨대, 종래 기술에서 설명한 「전송로 상에서의 데이터 오류를 정정 가능한 양자키 배송」에 상당하는 오류 정정 프로토콜)이면, 즉, 오류 정정 정보와 정보 m_A의 선형성이 확보되는 것이면, 그 행렬 H를 이용하는 것으로 해도 좋다.

여기서, 상기 패리티 검사 행렬 생성부(10)에서의 LDPC 부호의 구성법에 대하여, 상세하게는, 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」의 구성법(도 2 단계 S1의 상세)에 대하여 설명한다. 도 3은 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」의 구성법을 나타내는 흐름도이다. 또, 패리티 검사 행렬 생성부(30)에 대해서는, 패리티 검사 행렬 생성부(10)와 마찬가지로 동작하기 때문에 그 설명을 생략한다. 또한, 본 실시예에서의 검사 행렬 생성 처리는, 예컨대, 설정되는 파라미터에 따라 패리티 검사 행렬 생성부(10)로 실행하는 구성으로 해도 좋고, 통신 장치 외부의 다른 제어 장치(계산기 등)로 실행하는 것으로 해도 좋다. 본 실시예에서의 검사 행렬 생성 처리가 통신 장치 외부에서 실행되는 경우는, 생성 완료된 검사 행렬이 통신 장치에 저장된다. 이후의 실시예에서는, 패리티 검사 행렬 생성부(10)에서 상기 처리를 실행하는 경우에 대하여 설명한다.

우선, 패리티 검사 행렬 생성부(10)에서는, 「Irregular-LDPC 부호」용의 검사 행렬의 베이스로 되는 유한 아핀 기하 부호 AG(2, 2^s)를 선택한다(도 3, 단계 S21). 여기서는, 행의 가중치와 열의 가중치가 각각 2^s로 된다. 도 4는, 예컨대, 유한 아핀 기하 부호 AG(2, 2^2)의 매트릭스를 도시한 도면(공백은 0을 나타낸다)이다.

다음에, 패리티 검사 행렬 생성부(10)에서는, 열의 가중치의 최대값 $r_1(2<r_1\leq 2^s)$을 결정한다(단계 S22). 그리고, 부호화율(1-신드롬 길이/키의 길이)를 결정한다(단계 S22).

다음에, 패리티 검사 행렬 생성부(10)에서는, 가우스 근사법(Gaussian Approximation)에 의한 최적화를 이용하여, 잠정적으로, 열의 가중치 배분 $\lambda(\gamma_i)$와 행의 가중치 배분 ρ_u를 구한다(단계 S23). 또, 행의 가중치 배분의 생성함수 $\rho(x)$는 $\rho(x)=\rho_u x^{u-1}+(1-\rho_u)x^u$로 한다. 또한, 가중치 u는 $u\geq 2$의 정수이며, ρ_u는 행에서의 가중치 u의 비율을 나타낸다.

다음에, 패리티 검사 행렬 생성부(10)에서는, 유한 아핀 기하의 행의 분할에 의해 구성 가능한, 행의 가중치 {u, u+1}을 선택하고, 또한 (1)식을 만족시키는 분할 계수 $\{b_u, b_{u+1}\}$을 구한다(단계 S24). 또, b_u, b_{u+1}은 비부(非負)의 정수로 한다.

$$b_u+b_{u+1}(u+1)=2^s \quad \cdots (1)$$

구체적으로는, 하기 (2)식으로부터 b_u를 구하고, 상기 (1)식으로부터 b_{u+1}을 구한다.

$$\arg\cdot\min_{bu}\left|\varphi_u-\frac{u\times b_u}{2^s}\right| \quad \cdots (2)$$

다음에, 패리티 검사 행렬 생성부(10)에서는, 상기 결정한 파라미터 u, u+1, b_u, b_{u+1}에 의해(상기 행의 분할 처리에 의해) 갱신된 행의 가중치의 비율 ρ_u', ρ_{u+1}'을 (3)식에 의해 구한다(단계 S25).

$$\varphi'_u=\frac{u\times b_u}{2^s}$$
$$\varphi'_{u+1}=\frac{(u+1)\times b_{u+1}}{2^s} \quad \cdots (3)$$

다음에, 패리티 검사 행렬 생성부(10)에서는, 가우스 근사법에 의한 최적화를 이용하여, 또한 상기에서 구한 u, u+1, ρ_u', ρ_{u+1}'을 고정 파라미터로 하여, 잠정적으로 열의 가중치 배분 $\lambda(\gamma_i)$을 구한다(단계 S26). 또, 가중치 γ_i는 $\gamma_i\geq 2$의 정수이며, $\lambda(\gamma_i)$는 열에서의 가중치 γ_i의 비율을 나타낸다. 또한, 열수가 1 이하로 되는 가중치($\lambda(\gamma_i)\leq\gamma_i/w_t$, i는 정의 정수)를 후보에서 삭제한다. 단, w_t는 AG(2, 2^s)에 포함되는 1의 총수를 나타낸다.

다음에, 상기에서 구한 가중치 배분을 만족시키고, 또한 하기 (4)식을 만족시키는 열의 가중치 후보의 세트 $\{\gamma_1, \gamma_2, \cdots\gamma_l (\gamma_1 \leq 2^s)\}$를 선택한다(단계 S27). 그리고, 하기의 (4)식을 만족시키지 않는 열의 가중치 γ_i가 존재하는 경우에는, 그 열의 가중치를 후보로부터 삭제한다.

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,\ell} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,\ell} \\ \vdots & & \cdots & \vdots \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{bmatrix} = \begin{bmatrix} 2^s \\ 2^s \\ \vdots \\ 2^s \end{bmatrix} \quad \cdots \quad (4)$$

또, 각 a는, 열의 가중치 2^s를 구성하기 위한 $\{\gamma_1, \gamma_2, \cdots\gamma_l\}$에 대한 비부의 정수로 되는 계수를 나타내고, i, j는 정의 정수이며, γ_i는 열의 가중치를 나타내고, γ_1은 열의 최대가중치를 나타낸다.

다음에, 패리티 검사 행렬 생성부(10)에서는, 가우스 근사법에 의한 최적화를 이용하고, 또한 상기에서 구한 u, u+ 1, ρ_u', ρ_{u+1}'과 $\{\gamma_1, \gamma_2, \cdots\gamma_l\}$을 고정 파라미터로 하여, 열의 가중치 배분 $\lambda(\gamma_i)$과 행의 가중치 배분 ρ_u를 구한다(단계 S28).

다음에, 패리티 검사 행렬 생성부(10)에서는, 분할 처리를 하기 전에, 열의 가중치 배분 $\lambda(\gamma_i)$와 행의 가중치 배분 ρ_u를 조정한다(단계 S29). 또, 조정후의 각 가중치의 배분은, 가능한 한 가우스 근사법으로 구한 값에 가까운 값으로 한다. 도 5는 단계 S29에 있어서의 최종적인 열의 가중치 배분 $\lambda(\gamma_i)$와 행의 가중치 배분 ρ_u를 나타내는 도면이다.

마지막으로, 패리티 검사 행렬 생성부(10)에서는, 유한 아핀 기하에 있어서의 행 및 열을 분할하여(단계 S30), n×k의 패리티 검사 행렬 H를 생성한다. 본 발명에서의 유한 아핀 기하 부호의 분할 처리는, 규칙적으로 분할하는 것이 아니라, 각 행 또는 각 열에서 「1」의 번호를 랜덤하게 추출한다(후술하는 랜덤 분할의 구체예를 참조). 또, 이 추출 처리는, 랜덤성이 유지되는 것이면 어떠한 방법을 이용하여도 좋다.

구체적으로 말하면, EG(2, 2^5)에 있어서의 1열중의 「1」의 행 번호가,

$B_1(x)$ = {1 32 114 136 149 223 260 382 402 438 467 507 574 579 588 622
634 637 638 676 717 728 790 851 861 879 947 954 971 977 979 998}

인 경우, 분할 후의 행렬에서의 1~4열째 $R_m(n)$는, $B_1(x)$로부터 「1」의 번호가 랜덤하게 추출되고, 예컨대,

$R_1(n)$ = {1 114 574 637 851 879 977 979}
$R_2(n)$ = {32 136 402 467 588 728 861 971}
$R_3(n)$ = {149 260 382 438 579 638 717 998}
$R_4(n)$ = {223 507 622 634 676 790 947 954}

로 된다.

여기서, 상기 랜덤 분할의 일례, 즉, 상기 「난수 계열의 라틴 방진을 이용한 분할 방법」을 상세히 설명한다. 여기서는, 랜덤 분할을 하는 경우의 랜덤 계열을 용이하고 또한 확정적으로 생성한다. 이 방법에 의한 이점은, 송신측과 수신측이 동일한 랜덤 계열을 생성할 수 있는 것이다.

(1) 기본 랜덤 계열을 작성한다. 여기서는, 유한 아핀 기하 AG(2, 2^s)를 이용하여, P를 $P \geq 2^s$를 만족시키는 최소의 소수로 한 경우의, 기본 랜덤 계열 C(i)를 (5)식에 따라서 작성한다.

$$C(1) = 1$$
$$C(i+1) = G_0 \times C(i) \mod P \quad \cdots (5)$$

또, i=0, 1, …, P-2로 하고, G_0는 갈로아체 GF(P)의 원시원(原始元)이다. 또한, 계열 길이가 2^s가 되도록, 2^s보다 큰 수를 C(i)의 중에서 삭제하고, 삭제후의 C(i)를 기본의 랜덤 계열로 한다.

(2) 기본 랜덤 계열 C(i)를 일정 간격으로 판독하기 위해서 스킵 간격 S(j)를 이하의 (6)식과 같이 정의한다.

$$S(j)=j \quad j=1, 2, \cdots, 2^s \qquad \cdots (6)$$

(3) 이하의 (7)식으로 치환 패턴 $LB_j(i)$을 작성한다.

$$LB_j(i)=((S(j)\times i) \bmod P)+1$$
$$j=1, 2, \cdots, 2^s$$
$$i=1, 2, \cdots, P-1 \qquad \cdots (7)$$

또, LBj(i)도 2^s보다 큰 숫자는 삭제한다.

(4) q열 i행에서 j번째의 라틴 방진 행렬 $L_{jq}(i)$를 이하의 (8)식으로 산출한다.

$$L_{jq}(i)=LB_j(((q+i-2) \bmod 2^s)+1)$$
$$j=1, 2, \cdots, 2^s$$
$$i=1, 2, \cdots, 2^s$$
$$q=1, 2, \cdots, 2^s \qquad \cdots (8)$$

(5) 라틴 방진 행렬 $L_{jq}(i)$에 따라서 열과 행을 분할한다. 열의 분할로서는, g_0, g_0, …, g_{n+1}을 패리티 검사 행렬 H의 열벡터로 하고, $g_c'(k)$를 g_c, c=0, 1, …, n-1의 열의 중의 k번째의 「1」로 한다. 또한, g_c 중의 「1」의 위치의 집합을 G_c로 한다((9)식 참조).

$$G_c=\{g_c'(k), k=1, 2, \cdots, 2^s\} \qquad \cdots (9)$$

예컨대, AG(2, 2^3)의 c=1번째의 열의 「1」의 행 번호는, G_1={1 3 8 20 23 24 34 58}로 된다. 그리고, 이 c열째의 열벡터를 $g_c'(k)$로 표현하면, (10)식과 같이 나타낼 수 있다.

$$g_c'(1)=((c-1)+1) \bmod (2^{2s}-1)$$
$$g_c'(2)=(g_c'(1)+2) \bmod (2^{2s}-1)$$
$$g_c'(3)=(g_c'(2)+5) \bmod (2^{2s}-1)$$
$$g_c'(4)=(g_c'(3)+12) \bmod (2^{2s}-1)$$
$$g_c'(5)=(g_c'(4)+3) \bmod (2^{2s}-1)$$
$$g_c'(6)=(g_c'(5)+1) \bmod (2^{2s}-1)$$
$$g_c'(7)=(g_c'(6)+10) \bmod (2^{2s}-1)$$
$$g_c'(8)=(g_c'(7)+24) \bmod (2^{2s}-1) \qquad \cdots (10)$$

여기서, 패리티 검사 행렬 H의 각 열 g_c를, 상기 (4)식을 만족시키는 열의 차수와 계수에 근거하여, 새로운 열 $g_{c,e}$로 분할한다. 그리고, $g_{c,e}'(r)$를 새로운 열 $g_{c,e}$ 중의 r행째의 「1」로 한다. 또한, $g_{c,e}$의 중의 「1」의 위치의 집합을 $G_{c,e}$로 한다((11)식 참조).

$$G_{c,e}=\{g_{c,e}'(r), r=1, 2, \cdots\} \qquad \cdots (11)$$

그리고, 라틴 방진 행렬군을 이용하여, 하기 (12)식에 따라서 분할하는 에지의 선택을 한다. 또, $a_{t,1}$, $a_{t,2}$, …, $a_{t,l}$과 γ_1, γ_2, …, γ_l은, 상기 식(4)을 만족시키는 계수와 차수이다. 또한, t는 (4)식의 계수 행렬의 행 번호를 나타내고 있다. 또한, t행째의 식으로 분할하는 유한 아핀 평면의 열수를 n_t로 하고, 계수 행렬의 행 번호의 최대값을 t_m이라고 하면, t는 (13)식으로 나타낼 수 있다.

$$
\begin{aligned}
&g'_{c,e}(r) = g'_c(L_{j,q}(i)) \\
&j = c/2^s \\
&q = ((c-1) \bmod 2^s) + 1 \\
&i = r + \sum_{m=1}^{\ell} \min(a_{t,m}, \max(o, e-1-\sum_{n-1}^{m-1} a_{t,n})) \cdot \gamma_m
\end{aligned}
\quad \cdots (12)
$$

$$
t\begin{cases}
1 (1 \leqq c \leqq n_1) \\
2 (n_1+1 \leqq c \leqq n_1+n_2) \\
\quad \vdots \\
t_m (\sum_{i=1}^{tm-1} n_i + 1 \leqq c \leqq \sum_{i=2}^{tm} n_i)
\end{cases}
\quad \cdots (13)
$$

다음에, 상기 (1)~(4)의 분할 처리를, 구체예를 들어 설명한다. 예로서, AG(2, 2^3)의 c=16번째의 열의 「1」의 행 번호를 G_{16}={10 16 18 23 35 38 39 49}로 정의한다. 도 6은 랜덤 계열의 라틴 방진 행렬에 의한 분할 수순을 나타내는 도면이다. 도시한 라틴 방진 행렬 $L_{jq}(i)$의 결과를 이용하여 수순 (5)를 실행하면, 새로운 열 $g_{16,e}$ 중의 「1」은 (14)식과 같이 나타낼 수 있다.

$$
\begin{aligned}
&g_{16,1}'(1) = g_{16}'(L_{2,8}(1)) = g_{16}'(3) = 18 \\
&g_{16,1}'(2) = g_{16}'(L_{2,8}(2)) = g_{16}'(2) = 16 \\
&g_{16,2}'(1) = g_{16}'(L_{2,8}(3)) = g_{16}'(8) = 49 \\
&g_{16,2}'(2) = g_{16}'(L_{2,8}(4)) = g_{16}'(7) = 39 \\
&g_{16,3}'(1) = g_{16}'(L_{2,8}(5)) = g_{16}'(6) = 38 \\
&g_{16,3}'(2) = g_{16}'(L_{2,8}(6)) = g_{16}'(1) = 10 \\
&g_{16,4}'(1) = g_{16}'(L_{2,8}(7)) = g_{16}'(4) = 23 \\
&g_{16,4}'(2) = g_{16}'(L_{2,8}(8)) = g_{16}'(5) = 35
\end{aligned}
\quad \cdots (14)
$$

그 결과, 16번째의 열은 아래와 같이 분할된다.

$G_{16,1}$= {18 16}

$G_{16,2}$= {49 39}

$G_{16,3}$= {38 10}

$G_{16,4}$= {23 35}

이와 같이, 본 실시예에서는, 상기 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」의 구성법(도 2, 단계 S1)을 실행함으로써, 확정적이고 특성이 안정된 「Irregular-LDPC 부호」용의 검사 행렬 H(n×k)를 생성할 수 있다.

상기한 바와 같이, 패리티 검사 행렬 H, 생성 행렬 G, G^{-1}(G^{-1}·G=I:단위 행렬)을 생성한 후, 다음에, 송신측의 통신 장치에서는, 난수 발생부(11)가, 난수열(1, 0의 열: 송신 데이터)을 발생시키고, 또한 송신 코드(+ :수평수직 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드, ×:경사 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드)를 랜덤하게 결정한다(단계 S2). 한편, 수신측의 장치에서는, 난수 발생부(31)가 수신 코드(+ : 수평수직 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드, ×:경사 방향으로 편광된 광을 식별 가능한 측정기에 대응한 코드)를 랜덤하게 결정한다(단계 S12).

다음에, 송신측의 통신 장치에서는, 광자 생성부(12)가, 상기 난수열과 송신 코드의 조합에 의해 자동적으로 결정되는 편광 방향으로 광자를 송신한다(단계 S3). 예컨대, 0과 + 의 조합으로 수평 방향으로 편광된 광을, 1과 + 의 조합으로 수직 방향으로 편광된 광을, 0과 ×의 조합으로 45° 방향으로 편광된 광을, 1과 ×의 조합으로 135° 방향으로 편광된 광을, 양자 통신로에 각각 송신한다(송신 신호).

광자 생성부(12)에 의해 생성한 광 신호를 수취한 수신측의 통신 장치의 광자 수신부(32)에서는, 양자 통신로 상의 광을 측정한다(수신 신호). 그리고, 수신 코드와 수신 신호의 조합에 의해 자동적으로 결정되는 수신 데이터를 얻는다(단계 S13). 여기서는, 수신 데이터로서, 수평 방향으로 편광된 광과 + 의 조합으로 0을, 수직 방향으로 편광된 광과 + 의 조합으로 1을, 45° 방향으로 편광된 광과 ×의 조합으로 0을, 135° 방향으로 편광된 광과 ×의 조합으로 0을, 각각 얻는다.

다음에, 수신측의 통신 장치에서는, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하기 위해서, 난수 발생부(31)가, 수신 코드를, 공개 통신로를 거쳐서 송신측의 통신 장치에 대하여 송신한다(단계 S13). 수신 코드를 수취한 송신측의 통신 장치에서는, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하고, 그 결과를, 공개 통신로를 거쳐서 수신측의 통신 장치에 대하여 송신한다(단계 S3). 그리고, 수신측의 통신 장치 및 송신측의 통신 장치에서는, 정확한 측정기로 수신한 수신 신호에 대응하는 데이터만을 남기고, 그 이외의 것을 버린다(단계 S3, S13). 그 후, 남은 데이터를 메모리 등에 보존하고, 그 선두부터 순서대로 n 비트를 판독하고, 송신 데이터 m_A와 수신 데이터 m_B(m_B는 전송로 상에서 잡음 등의 영향을 받은 m_A)를 생성한다. 즉, 여기서는, 공유키 생성 처리가 끝날 때에 다음의 n 비트를 판독하고, 그 때마다, 송신 데이터 m_A와 수신 데이터 m_B를 생성한다. 본 실시예에서는, 정확한 측정기로 수신한 수신 신호에 대응하는 비트의 위치를 송신측의 통신 장치와 수신측의 통신 장치 사이에서 공유할 수 있다.

다음에, 송신측의 통신 장치에서는, 신드롬 생성부(14)가, 패리티 검사 행렬 H(n×k)와 송신 데이터 m_A를 이용하여 m_A의 신드롬 $S_A=Hm_A$를 계산하고, 그 결과를, 공개 통신로 통신부(13), 공개 통신로를 거쳐서 수신측의 통신 장치에 통지한다(단계 S4). 이 단계에서, m_A의 신드롬 S_A(k비트분의 정보)는 도청자에게 알려질 가능성이 있다. 한편, 수신측의 통신 장치에서는, 공개 통신로 통신부(34)에서 m_A의 신드롬 S_A를 수신하고, 그것을 신드롬 복호부(33)에 통지한다(단계 S14).

신드롬 복호부(33)에서는, 패리티 검사 행렬 H와 수신 데이터 m_B를 이용하여 m_B의 신드롬 $S_B=Hm_B$를 계산하고, 또한, m_A의 신드롬 S_A와 m_B의 신드롬 S_B를 이용하여 신드롬 $S=S_A+S_B$를 계산한다(단계 S15). 그리고, 신드롬 S에 근거하여 송신 데이터 m_A를 추정한다(단계 S16). 여기서는, $m_B=m_A+e$(잡음 등)로 가정하여, 식 (15)에 나타내는 바와 같이 신드롬 S를 변형한 후, 신드롬 복호에 의해 e를 구하고, 송신 데이터 m_A를 구한다(단계 S16). 또, S_A+S_B, m_A+e의 +는 배타적 논리합을 나타낸다.

$$
\begin{aligned}
S &= S_A + S_B \\
&= Hm_A + Hm_B \\
&= H\,(m_A + m_B) \\
&= H\,(m_A + m_A + e) \\
&= He \qquad \cdots (15)
\end{aligned}
$$

마지막으로, 수신측의 통신 장치에서는, 공유키 생성부(35)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보(m_A)의 일부를 버리고, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S17).

즉, 공유키 생성부(35)에서는, 먼저 계산해 놓은 $G^{-1}(n\times(n-k))$을 이용하여 하기 (16)식에 의해 암호키 r을 생성한다. 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

$$r = G^{-1}m_A \qquad \cdots (16)$$

한편, 송신측의 통신 장치에서도, 공유키 생성부(15)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보(m)의 일부를 버리고, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S5). 즉, 공유키 생성부(15)에서는, 먼저 계산해 놓은 $G^{-1}(n\times(n-k))$을 이용하여 상기 (16)식에 의해 암호키 r을 생성한다(단계 S5). 송신측의 통신 장치는 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

이와 같이, 본 실시예에서는, 확정적이고 특성이 안정된 「Irregular-LDPC 부호」용의 패리티 검사 행렬을 이용하여 공유 정보의 데이터 오류를 정정하고, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버리는 구성으로 했다. 이에 따라, 오류 비트를 특정/정정하기 위한 방대한 회수의 패리티의 교환이 없어지고, 오류 정정 정보를 송신하는 것만으로 오류 정정 제어가 행하여지기 때문에, 오류 정정 처리에 걸리는 시간을 대폭 단축 가능하다. 또한, 공개된 정보에 따라 공유 정보의 일부를 버리고 있기 때문에, 고도로 안전성이 보증된 공통키를 생성할 수 있다.

또, 본 실시예에서는, HG=0을 만족시키는 생성 행렬 G((n-k)×n)로부터, $G^{-1}\cdot G=I$(단위 행렬)로 되는 역행열 G^{-1}(n×(n-k))을 생성하고, 당해 역행열 G^{-1}을 이용하여 공유 정보(n)의 일부(k)를 버리고, n-k 비트분의 정보량을 구비한 암호키 r을 생성하는 것으로 했지만, 이것에 한정되지 않고, 공유 정보(n)의 일부를 버리고, m(m≤n-k) 비트분의 정보량을 구비한 암호키 r을 생성하는 것으로 해도 좋다. 구체적으로 말하면, n차원 벡터를 m차원 벡터에 맵핑하는 사상(寫像) F(·)를 상정한다. F(·)는, 공유키의 안전성을 보증하기 위해서, 「임의의 m차원 벡터 v에 대하여, 사상 F와 생성 행렬 G의 합성 사상 F·G에서의 역상(逆像)$(F\cdot G)^{-1}(v)$의 본래의 개수가 v에 상관없이 일정(2^{n-k-m})하다」라는 조건을 만족시킬 필요가 있다. 이 때, 공유키 r은, $r=F(m_A)$로 된다.

(실시예 2)

실시예 2에서는, 상술한 실시예 1에 있어서의 암호키의 비닉성을 더 증강시킨다.

도 7은 본 발명에 따른 양자 암호 시스템의 실시예 2의 구성을 나타내는 도면이다. 또, 먼저 설명한 실시예 1과 동일한 구성에 대해서는, 동일한 부호를 부여하고 그 설명을 생략한다. 양자 통신로에서 도청된 정보에 대하여 비닉성을 증강시키기 위해서는, 도청된 비트수분을 해쉬함수에 의해 압축해야 한다. 그러나, 해쉬함수는 그 특성에 의해 도청되기 쉬운 위치가 존재한다. 그래서, 본 실시예에 있어서는, 그 위치를 랜덤하게 치환하는 것에 따라 대응한다.

도 8은 실시예 2의 양자키 배송을 나타내는 흐름도이며, 상세하게는, 송신측의 통신 장치의 처리를 나타낸다. 송신측의 통신 장치의 랜덤 치환부(16)에서는, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 생성하며, 당해 R을 공유키 생성부(15)에 통지하고, 또한, 당해 R을, 공개 통신로를 거쳐서 수신측의 통신 장치의 공유키 생성부(35)에 통지한다(단계 S6). 또, 도 7 및 도 8에서는, 일례로서, 송신측의 통신 장치로 랜덤 행렬 R을 생성/송신하고 있지만, 이것에 한정되지 않고, 이 처리는 수신측의 통신 장치로 실행하는 것으로 해도 좋다.

그 후, 송신측의 통신 장치에서는, 공유키 생성부(15)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보(m_A)의 일부를 버리고, 또한, 수취한 랜덤 행렬 R을 이용하여 비닉성을 증강하여, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S5). 즉, 공유키 생성부(15)에서는, 먼저 계산해 놓은 G^{-1}(n×(n-k))와 수취한 랜덤 행렬 R((n-k)×(n-k))을 이용하여 하기 (17)식에 의해 암호키 r을 생성한다. 송신측의 통신 장치는 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

$$r = R G^{-1} m_A \qquad \cdots (17)$$

한편, 수신측의 통신 장치에서도, 공유키 생성부(35)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보(m_A)의 일부를 버리고, 또한, 수취한 랜덤 행렬 R을 이용하여 비닉성을 증강하여, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S17). 즉, 공유키 생성부(15)에서는, 먼저 계산해 놓은 G^{-1}(n×(n-k))와 수취한 랜덤 행렬 R((n-k)×(n-k))을 이용하여 상기 (17)식에 의해 암호키 r을 생성한다(단계 S17). 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

이와 같이, 본 실시예에서는, 확정적이고 특성이 안정된 「Irregular-LDPC 부호」용의 패리티 검사 행렬을 이용하여 공유 정보의 데이터 오류를 정정하고, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버리고, 또한 정칙인 랜덤 행렬을 이용하여 공유 정보를 치환하는 구성으로 했다. 이에 따라, 오류 비트를 특정/정정하기 위한 방대한 회수의 패리티의 교환이 없어지고, 오류 정정 정보를 송신하는 것만으로 오류 정정 제어가 행하여지기 때문에, 오류 정정 처리에 걸리는 시간을 대폭 단축할 수 있다. 또한, 공개된 정보에 따라 공유 정보의 일부를 버리고 있기 때문에, 고도로 안전성이 보증된 공통키를 생성할 수 있다. 또한, 정칙인 랜덤 행렬을 이용하여 공유 정보를 치환하는 것으로 했기 때문에, 비닉성을 증강시킬 수 있다.

또, 본 실시예에 있어서도, 실시예 1과 마찬가지로, 공유 정보(n)의 일부를 버리고, m(m≤n-k) 비트분의 정보량을 구비한 암호키 r을 생성하는 것으로 해도 좋다. 이 경우, 공유키 r은, $r=RF(m_A)$로 된다.

(실시예 3)

먼저 설명한 실시예 1에서는, 생성 행렬 G^{-1}을 이용하여 공유 정보의 일부를 버리고 있었다. 이것에 대하여, 실시예 3에서는, 생성 행렬 G^{-1}을 이용하지 않고, 패리티 검사 행렬 H의 특성을 이용하여 공유 정보의 일부를 버린다. 또, 본 실시예의 구성은, 먼저 설명한 실시예 1의 도 1과 마찬가지다.

이하, 실시예 3의 양자키 배송에 대하여 설명한다. 여기서는, 먼저 설명한 도 2와 다른 처리에 대해서만 설명한다.

우선, 상기 송신측의 통신 장치 및 수신측의 통신 장치에서는, 패리티 검사 행렬 생성부(10, 30)가 특정 선형 부호의 패리티 검사 행렬 H(n×k)를 구한다(단계 S1, 단계 S11). 또, 유한 아핀 기하에 근거한 「Irregular-LDPC 부호」의 구성법(도 2 단계 S1의 상세)에 대해서는, 먼저 설명한 실시예 1의 도 3과 마찬가지다.

그리고, 실시예 1과 마찬가지의 수순으로 단계 S2~S4를 실행 후, 수신측의 통신 장치에서는, 공유키 생성부(35)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보(m_A)의 일부를 버리고, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S17). 구체적으로는, 공유키 생성부(35)가, 상기 단계 S11에서 생성한 패리티 검사 행렬의 열에 대하여 랜덤 치환을 한다. 그리고, 송신측의 통신 장치와의 사이에서 버리는 비트에 관한 정보를, 공개 통신로를 거쳐서 교환한다. 여기서는, 본래의 유한 아핀 기하 $AG(2, 2^s)$의 1열째 중에서 특정 「1」을 선택하고, 그 위치를, 공개 통신로를 거쳐서 교환한다.

그 후, 공유키 생성부(35)에서는, 상기 치환 후의 패리티 검사 행렬로부터 상기 「1」에 대응하는 분할 후의 위치, 및 순회 시프트된 각 열에서의 상기 「1」에 대응하는 분할 후의 위치를 특정하고, 그 특정한 위치에 대응하는 공유 정보 m_A 내의 비트를 버리고, 나머지의 데이터를 암호키 r로 한다. 수신측의 통신 장치는, 이 암호키 r을 송신측의 통신 장치와의 공유키로 한다.

한편, 송신측의 통신 장치에서도, 공유키 생성부(15)가, 공개된 오류 정정 정보(도청되었을 가능성이 있는 상기 k 비트분의 정보: S_A)에 따라 공유 정보(m_A)의 일부를 버리고, n-k 비트분의 정보량을 구비한 암호키 r을 생성한다(단계 S5). 구체적으로는, 공유키 생성부(15)가, 상기 단계 S1에서 생성한 패리티 검사 행렬의 열에 대하여 상기와 동일한 랜덤 치환을 한다. 그리고, 상기 버리는 비트에 관한 정보를, 공개 통신로를 거쳐서 교환한다.

그 후, 공유키 생성부(15)에서는, 상기 치환 후의 패리티 검사 행렬로부터 상기 「1」에 대응하는 분할 후의 위치, 및 순회 시프트된 각 열에서의 상기 「1」에 대응하는 분할 후의 위치를 특정하고, 그 특정한 위치에 대응하는 공유 정보 m_A 내의 비트를 버리고, 나머지의 데이터를 암호키 r로 한다. 송신측의 통신 장치는 이 암호키 r을 수신측의 통신 장치와의 공유키로 한다.

이와 같이, 본 실시예에 있어서는, 생성 행렬 G^{-1}을 이용하지 않고, 패리티 검사 행렬 H의 특성을 이용하여 공유 정보의 일부를 버리는 구성으로 했다. 이에 따라, 실시예 1과 동일한 효과를 얻을 수 있고, 또한, 복잡한 생성 행렬 G, G^{-1}의 연산 처리를 삭제할 수 있다.

또, 본 실시예에서는, 패리티 검사 행렬 H의 특성을 이용하여 공유 정보의 일부를 버리고, 또한, 실시예 2와 마찬가지로, 정칙인 랜덤 행렬을 이용하여 공유 정보를 치환하는 구성으로 해도 좋다. 이에 따라, 비닉성을 증강시킬 수 있다.

이상, 설명한 바와 같이, 본 발명에 따르면, 확정적이고 특성이 안정된 「Irregular-LDPC 부호」용의 패리티 검사 행렬을 이용하여 공유 정보의 데이터 오류를 정정하고, 공개된 오류 정정 정보에 따라 공유 정보의 일부를 버리는 것으로 했다. 이에 따라, 오류 비트를 특정/정정하기 위한 방대한 회수의 패리티의 교환이 없어지고, 오류 정정 정보를 송신하는 것만으로 오류 정정 제어가 행하여지기 때문에, 오류 정정 처리에 걸리는 시간을 대폭 단축할 수 있다는 효과가 있다. 또한, 공개된 정보에 따라 공유 정보의 일부를 버리고 있기 때문에, 고도로 안전성이 보증된 공통키를 생성할 수 있다는 효과가 있다.

산업상 이용 가능성

이상과 같이, 본 발명에 따른 양자키 배송 방법 및 통신 장치는 통신 매체로서 광자를 이용한 양자 암호 시스템에 유용하며, 특히, 고도로 안전성이 보증된 공통키를 생성하기 위한 장치로서 적합하다.

청구의 범위

청구항 1.

광자(光子)를 양자 통신로 상에 송신하는 제 1 통신 장치와 당해 광자를 측정하는 제 2 통신 장치로 구성된 양자 암호 시스템에서의 양자키 배송 방법에 있어서,

상기 제 1 및 제 2 통신 장치가, 동일한 패리티 검사 행렬 H(n×k)를 생성하는 검사 행렬 생성 단계와,

상기 제 1 통신 장치가, 난수열(송신 데이터)을 발생시키고, 또한 소정의 송신 코드(기저)를 랜덤하게 결정하고, 상기 제 2 통신 장치가, 소정의 수신 코드(기저)를 랜덤하게 결정하는 난수 발생 단계와,

상기 제 1 통신 장치가, 상기 송신 데이터와 송신 코드의 조합에 의해 규정된 양자 상태에서, 광자를 양자 통신로 상에 송신하는 광자 송신 단계와,

상기 제 2 통신 장치가, 양자 통신로 상의 광자를 측정하고, 상기 수신 코드와 측정 결과의 조합에 의해 규정된 수신 데이터를 얻는 광자 수신 단계와,

상기 제 1 및 제 2 통신 장치가, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하여, 정확한 측정기로 측정된 n 비트의 수신 데이터 및 대응하는 송신 데이터를 남기고, 그 이외의 것을 버리는 데이터 삭제 단계와,

상기 제 1 통신 장치가, 상기 패리티 검사 행렬 H와 n 비트의 송신 데이터에 근거한 k 비트의 오류 정정 정보를, 공개 통신로를 거쳐서 상기 제 2 통신 장치에 통지하는 오류 정정 정보 통지 단계와,

상기 제 2 통신 장치가, 상기 패리티 검사 행렬 H와 n 비트의 수신 데이터와 오류 정정 정보에 근거하여, 수신 데이터의 오류를 정정하는 오류 정정 단계와,

상기 제 1 및 제 2 통신 장치가, 공개된 오류 정정 정보에 따라 오류 정정 후의 공유 정보(n)의 일부(k)를 버리고, 나머지 정보로 암호키를 생성하여, 이 암호키를 장치간의 공유키로 하는 암호키 생성 단계

를 포함하는 것을 특징으로 하는 양자키 배송 방법.

청구항 2.

제 1 항에 있어서,

상기 검사 행렬 생성 단계에서는,

기본 행렬로서 유한 아핀 기하(finite affine geometry)를 이용하여, 가우스 근사법에 의한 최적화를 함으로써, 패리티 검사 행렬의 최적의 행과 열의 가중치 배분을 탐색하는 가중치 탐색 단계와,

상기 최적의 가중치 배분에 근거하여, 상기 유한 아핀 기하의 행 및 열의 가중치를 소정의 수순에 의해 랜덤하게 분할하고, 열과 행의 가중치 또는 어느 한쪽이 균일하지 않은 저밀도 패리티 검사 부호의 패리티 검사 행렬 H를 생성하는 분할 단계

를 포함하는 것을 특징으로 하는 양자키 배송 방법.

청구항 3.

제 1 항에 있어서,

상기 검사 행렬 생성 단계에서는, 또한, 「HG=0」을 만족시키는 생성 행렬 G((n-k)×n)로부터, G^{-1}·G=I(단위 행렬)로 되는 역행열 G^{-1}(n×(n-k))을 생성하고,

상기 암호키 생성 단계에서는, 역행열 G^{-1}을 이용하여 공유 정보(n)의 일부(k)를 버리는 것

을 특징으로 하는 양자키 배송 방법.

청구항 4.

제 3 항에 있어서,

상기 암호키 생성 단계에서는, 상기 공유 정보(n)의 일부(k)를 버린 후, 한쪽의 장치가 정칙인 랜덤 행렬 R((n-k)×(n-k))을 생성하고, 공개 통신로를 거쳐서 다른 쪽의 통신 장치에 통지하며, 상기 제 1 및 제 2 통신 장치가, 각각 상기 랜덤 행렬 r을 암호키에 작용시키는 것을 특징으로 하는 양자키 배송 방법.

청구항 5.

제 1 항에 있어서,

상기 검사 행렬 생성 단계에서는, 또한, n차원 벡터를 m(m≤n-k)차원 벡터에 맵핑하는 사상(寫像) F에서, 임의의 m차원 벡터 v에 대하여, 사상 F와 「HG=0」을 만족시키는 생성 행렬 G의 합성 사상 F·G에서의 역상$(F\cdot G)^{-1}$(v)의 본래의 개수가 v에 상관없이 일정(2^{n-k-m})인 것을 생성하고,

상기 암호키 생성 단계에서는, 사상 F를 이용하여 공유 정보(n)의 일부를 버리는

것을 특징으로 하는 양자키 배송 방법.

청구항 6.

제 5 항에 있어서,

상기 암호키 생성 단계에서는, 상기 공유 정보(n)의 일부(k)를 버린 후, 한쪽의 장치가, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 생성하고, 공개 통신로를 거쳐서 다른 쪽의 통신 장치에 통지하며, 상기 제 1 및 제 2 통신 장치가, 각각 상기 랜덤 행렬 r을 암호키에 작용시키는 것을 특징으로 하는 양자키 배송 방법.

청구항 7.

제 2 항에 있어서,

상기 암호키 생성 단계에서는, 상기 패리티 검사 행렬 H의 열에 대하여 랜덤 치환을 실행하고, 상기 패리티 검사 행렬 H의 생성원의 유한 아핀 기하 AG(2, 2^s)의 1열째 중에서 특정 「1」을 선택하고, 그 위치를, 공개 통신로를 거쳐서 교환하며,

상기 치환 후의 패리티 검사 행렬로부터 상기 「1」에 대응하는 분할 후의 위치(열), 및 순회 시프트된 각 열에서의 상기 「1」에 대응하는 분할 후의 위치(열)를 특정하며, 그 특정한 위치(열)에 대응하는 공유 정보(n)의 일부(k)를 버리는 것을 특징으로 하는 양자키 배송 방법.

청구항 8.

제 7 항에 있어서,

상기 암호키 생성 단계에서는, 상기 공유 정보(n)의 일부(k)를 버린 후, 한쪽의 장치가, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 생성하고, 공개 통신로를 거쳐서 다른 쪽의 통신 장치에 통지하며, 상기 제 1 및 제 2 통신 장치가, 각각 상기 랜덤 행렬 R을 암호키에 작용시키는 것을 특징으로 하는 양자키 배송 방법.

청구항 9.

광자를 양자 통신로 상에 송신하는 통신 장치에 있어서,

수신측의 통신 장치와 동일한 패리티 검사 행렬 H(n×k)를 생성하는 검사 행렬 생성 수단과,

난수열(송신 데이터)을 발생시키고, 소정의 송신 코드(기저)를 랜덤하게 결정하고, 당해 송신 데이터와 송신 코드의 조합에 의해 규정된 양자 상태로 광자를 양자 통신로 상에 송신하며, 그 후, 상기 수신측의 통신 장치에서의 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하여, 정확한 측정기로 측정된 n 비트의 송신 데이터를 남기고, 그 이외의 것을 버리는 송신 수단과,

상기 패리티 검사 행렬 H와 n 비트의 송신 데이터에 근거한 k 비트의 오류 정정 정보를, 공개 통신로를 거쳐서 상기 수신측의 통신 장치에 통지하는 오류 정정 정보 통지 수단과,

공개한 오류 정정 정보에 따라 오류 정정 후의 공유 정보(n)의 일부(k)를 버리고, 나머지 정보로 암호키를 생성하여, 이 암호키를 수신측의 통신 장치와의 공유키로 하는 암호키 생성 수단

을 구비하는 것을 특징으로 하는 통신 장치.

청구항 10.

제 9 항에 있어서,

상기 검사 행렬 생성 수단은,

기본 행렬로서 유한 아핀 기하를 이용하여, 가우스 근사법에 의한 최적화를 함으로써, 패리티 검사 행렬의 최적의 행과 열의 가중치 배분을 탐색하고,

상기 최적의 가중치 배분에 근거하여, 상기 유한 아핀 기하의 행 및 열의 가중치를 소정의 수순에 의해 랜덤하게 분할하며,

열과 행의 가중치 또는 어느 한쪽이 균일하지 않은 저밀도 패리티 검사 부호의 패리티 검사 행렬 H를 생성하는

것을 특징으로 하는 통신 장치.

청구항 11.

제 9 항에 있어서,

상기 검사 행렬 생성 수단은, 「HG=0」을 만족시키는 생성 행렬 G((n-k)×n)로부터, G^{-1}·G=I(단위 행렬)로 되는 역행렬 G^{-1}(n×(n-k))을 더 생성하고,

상기 암호키 생성 수단은, 역행열 G^{-1}을 이용하여 공유 정보(n)의 일부(k)를 버리는

것을 특징으로 하는 통신 장치.

청구항 12.

제 11 항에 있어서,

상기 암호키 생성 수단은, 상기 공유 정보(n)의 일부(k)를 버린 후, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 상기 암호키에 작용시키는 것을 특징으로 하는 통신 장치.

청구항 13.

제 9 항에 있어서,

상기 검사 행렬 생성 수단은, n차원 벡터를 m(m≤n-k)차원 벡터에 맵핑하는 사상 F에서, 임의의 m차원 벡터 v에 대하여, 사상 F와 「HG=0」을 만족시키는 생성 행렬 G의 합성 사상 F·G에서의 역상$(F\cdot G)^{-1}$(v)의 본래의 개수가 v에 상관없이 일정(2^{n-k-m})인 것을 더 생성하고,

상기 암호키 생성 수단은, 사상 F를 이용하여 공유 정보(n)의 일부를 버리는

것을 특징으로 하는 통신 장치.

청구항 14.

제 13 항에 있어서,

상기 암호키 생성 수단은, 상기 공유 정보(n)의 일부(k)를 버린 후, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 상기 암호키에 작용시키는 것을 특징으로 하는 통신 장치.

청구항 15.

제 10 항에 있어서,

상기 암호키 생성 수단에 있어서는, 상기 패리티 검사 행렬 H의 열에 대하여 랜덤 치환을 실행하고, 상기 패리티 검사 행렬 H의 생성원의 유한 아핀 기하 $AG(2, 2^s)$의 1열째 중에서 특정 「1」을 선택하고, 그 위치를, 공개 통신로를 거쳐서 교환하며, 상기 치환 후의 패리티 검사 행렬로부터 상기 「1」에 대응하는 분할 후의 위치(열), 및 순회 시프트된 각 열에서의 상기 「1」에 대응하는 분할 후의 위치(열)를 특정하고, 그 특정한 위치(열)에 대응하는 공유 정보(n)의 일부(k)를 버리는 것을 특징으로 하는 통신 장치.

청구항 16.

제 15 항에 있어서,

상기 암호키 생성 수단은, 상기 공유 정보(n)의 일부(k)를 버린 후, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 상기 암호키에 작용시키는 것을 특징으로 하는 통신 장치.

청구항 17.

양자 통신로 상의 광자를 측정하는 통신 장치에 있어서,

송신측의 통신 장치와 동일한 패리티 검사 행렬 H(n×k)를 생성하는 검사 행렬 생성 수단과,

소정의 수신 코드(기저)를 랜덤하게 결정하고, 양자 통신로 상의 광자를 측정하여, 상기 수신 코드와 측정 결과의 조합에 의해 규정된 수신 데이터를 재생하며, 그 후, 상기 측정이 정확한 측정기로 행하여진 것인지 여부를 조사하여, 정확한 측정기로 측정된 n 비트의 수신 데이터를 남기고, 그 이외의 것을 버리는 수신 수단과,

공개 통신로를 거쳐서 수신한 k 비트의 오류 정정 정보와, 상기 패리티 검사 행렬 H와 n 비트의 수신 데이터에 근거하여, 수신 데이터의 오류를 정정하는 오류 정정 수단과,

공개된 오류 정정 정보에 따라 오류 정정 후의 공유 정보(n)의 일부(k)를 버리고, 나머지 정보로 암호키를 생성하며, 이 암호키를 송신측의 통신 장치와의 공유키로 하는 암호키 생성 수단

을 구비하는 것을 특징으로 하는 통신 장치.

청구항 18.

제 17 항에 있어서,

상기 검사 행렬 생성 수단은,

기본 행렬로서 유한 아핀 기하를 이용하여, 가우스 근사법에 의한 최적화를 함으로써, 패리티 검사 행렬의 최적의 행과 열의 가중치 배분을 탐색하고,

상기 최적의 가중치 배분에 근거하여, 상기 유한 아핀 기하의 행 및 열의 가중치를 소정의 수순에 의해 랜덤하게 분할하며,

열과 행의 가중치 또는 어느 한쪽이 균일하지 않은 저밀도 패리티 검사 부호의 패리티 검사 행렬 H를 생성하는

것을 특징으로 하는 통신 장치.

청구항 19.

제 17 항에 있어서,

상기 검사 행렬 생성 수단은, 또한, 「HG=0」을 만족시키는 생성 행렬 G((n-k)×n)로부터, $G^{-1}\cdot G=I$(단위 행렬)로 되는 역행열 G^{-1}(n×(n-k))을 생성하고,

상기 암호키 생성 수단은, 역행열 G^{-1}을 이용하여 공유 정보(n)의 일부(k)를 버리는

것을 특징으로 하는 통신 장치.

청구항 20.

제 19 항에 있어서,

상기 암호키 생성 수단은, 상기 공유 정보(n)의 일부(k)를 버린 후, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 상기 암호키에 작용시키는 것을 특징으로 하는 통신 장치.

청구항 21.

제 17 항에 있어서,

상기 검사 행렬 생성 수단은, n차원 벡터를 m(m≤n-k)차원 벡터에 맵핑하는 사상 F에서, 임의의 m차원 벡터 v에 대하여, 사상 F와 「HG=0」을 만족시키는 생성 행렬 G의 합성 사상 F·G에서의 역상$(F, G)^{-1}(v)$의 본래의 개수가 v에 상관없이 일정(2^{n-k-m})한 것을 더 생성하고,

상기 암호키 생성 수단은 사상 F를 이용하여 공유 정보(n)의 일부를 버리는

것을 특징으로 하는 통신 장치.

청구항 22.

제 21 항에 있어서,

상기 암호키 생성 수단은, 상기 공유 정보(n)의 일부(k)를 버린 후, 정칙인 랜덤 행렬 R((n-k)×(n-k))을 상기 암호키에 작용시키는 것을 특징으로 하는 통신 장치.

청구항 23.

제 18 항에 있어서,

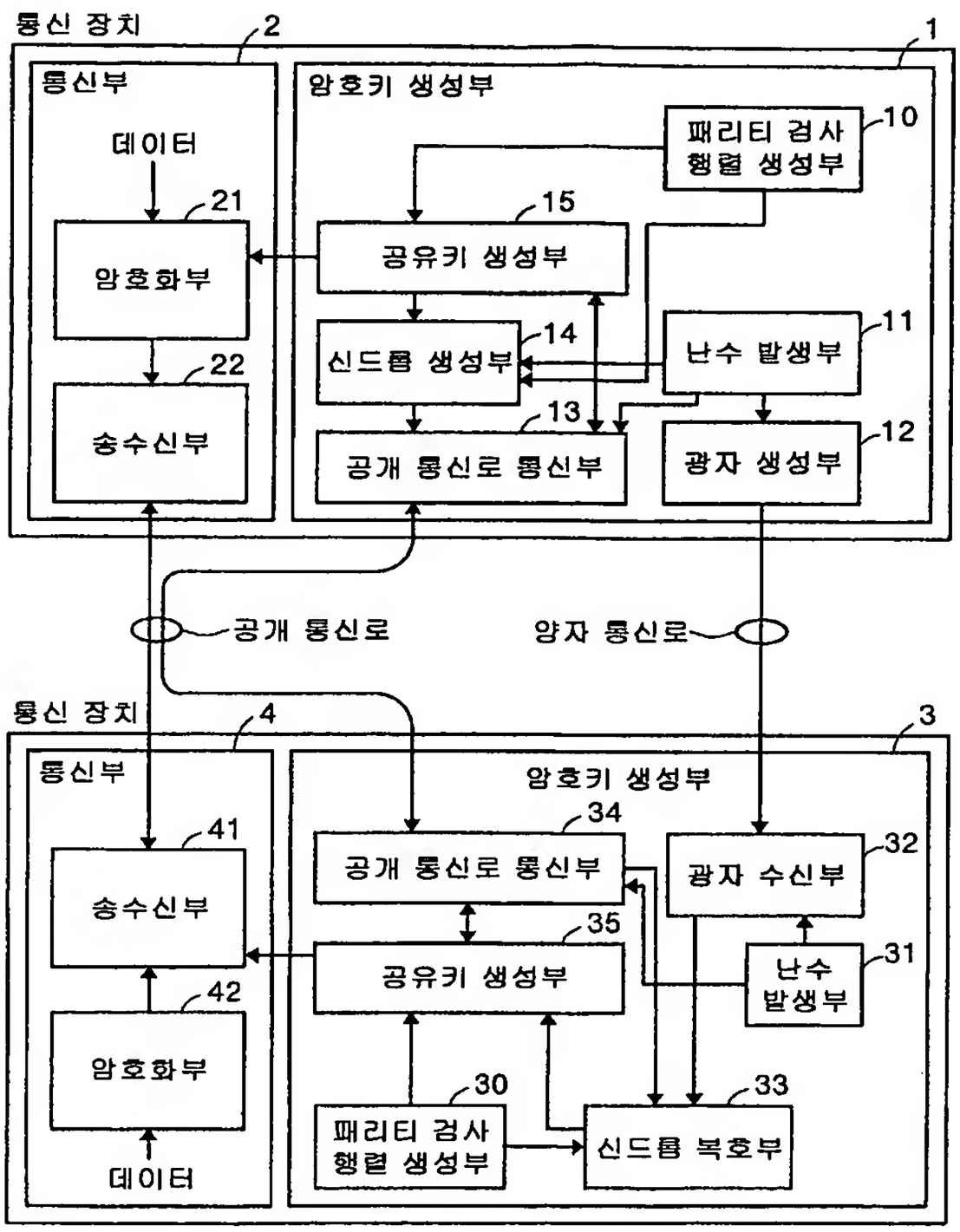
상기 암호키 생성 수단에서는, 상기 패리티 검사 행렬 H의 열에 대하여 랜덤 치환을 실행하며, 상기 패리티 검사 행렬 H의 생성원의 유한 아핀 기하 $AG(2, 2^s)$의 1열째 중에서 특정 「1」을 선택하고, 그 위치를, 공개 통신로를 거쳐서 교환하며, 상기 치환 후의 패리티 검사 행렬로부터 상기 「1」에 대응하는 분할 후의 위치(열), 및 순회 시프트된 각 열에서의 상기 「1」에 대응하는 분할 후의 위치(열)를 특정하고, 그 특정한 위치(열)에 대응하는 공유 정보(n)의 일부(k)를 버리는 것을 특징으로 하는 통신 장치.

청구항 24.

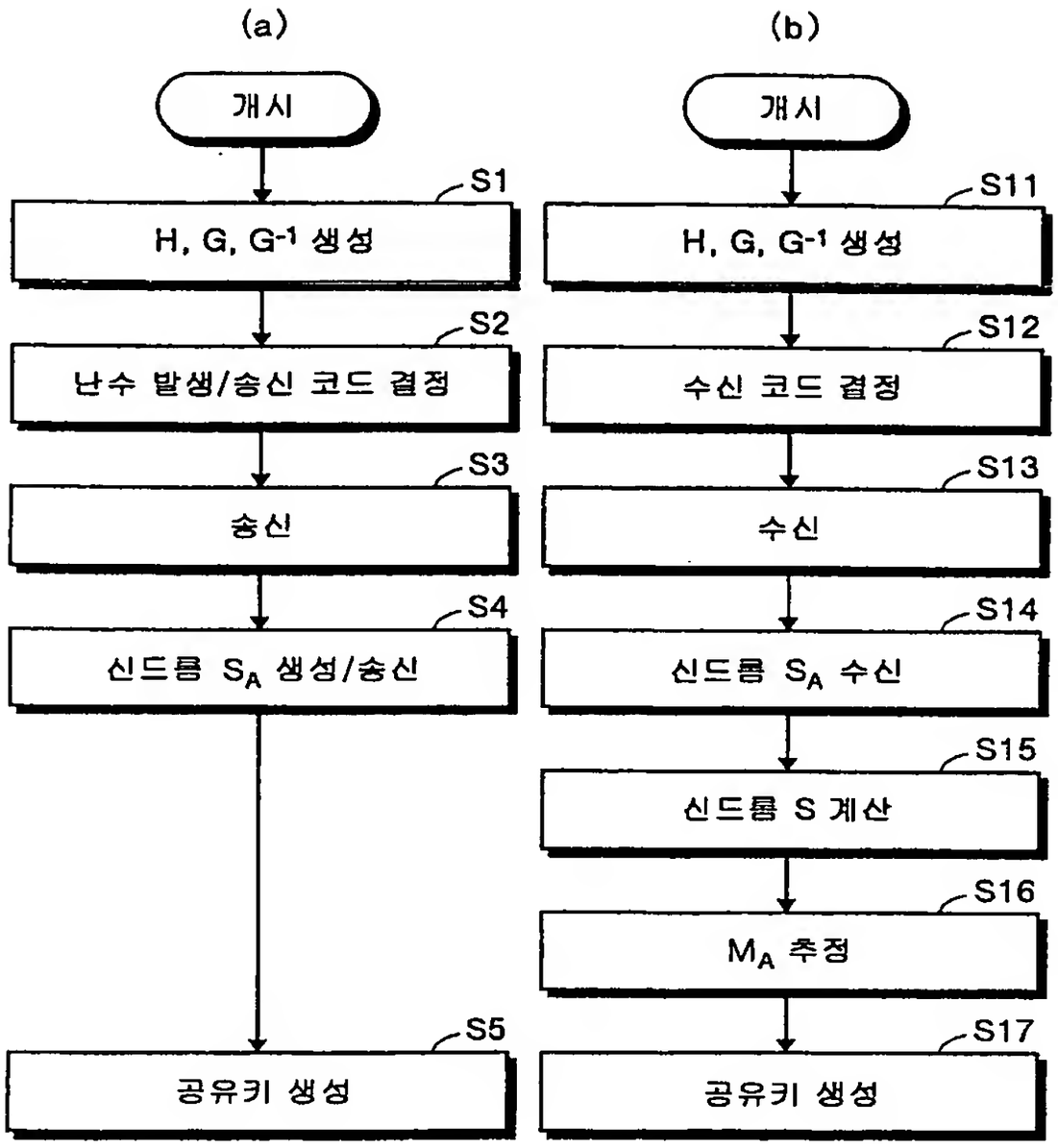
제 23 항에 있어서,

상기 암호키 생성 수단은, 상기 공유 정보(n)의 일부(k)를 버린 후, 정칙인 랜덤 행렬 R((n-k)××-k))을 상기 암호키에 작용시키는 것을 특징으로 하는 통신 장치.

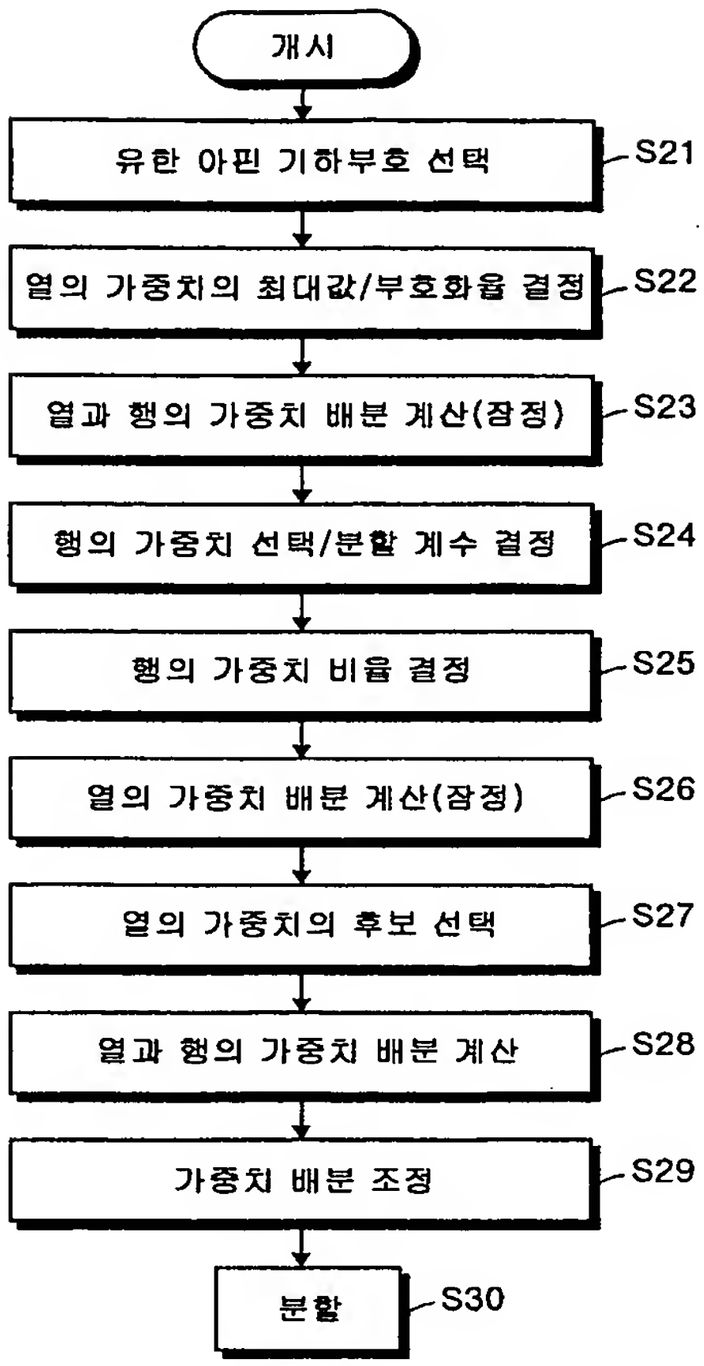
도면1


통신 장치
2
1
통신부
데이터
21
암호화부
22
송수신부
암호키 생성부
패리티 검사
행렬 생성부
10
15
공유키 생성부
14
신드롬 생성부
난수 발생부
11
13
공개 통신로 통신부
광자 생성부
12
공개 통신로
양자 통신로
통신 장치
4
3
통신부
41
송수신부
42
암호화부
데이터
암호키 생성부
34
공개 통신로 통신부
광자 수신부
32
35
공유키 생성부
난수
발생부
31
30
33
패리티 검사
행렬 생성부
신드롬 복호부

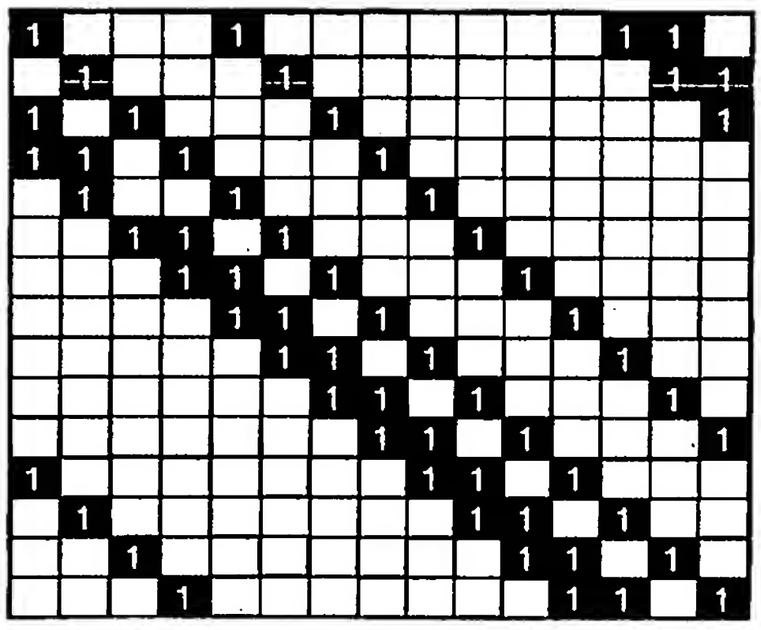
도면2


(a)
개시
S1
H, G, G-1 생성
S2
난수 발생/송신 코드 결정
S3
송신
S4
신드롬 SA 생성/송신
S5
공유키 생성
(b)
개시
S11
H, G, G-1 생성
S12
수신 코드 결정
S13
수신
S14
신드롬 SA 수신
S15
신드롬 S 계산
S16
MA 추정
S17
공유키 생성

도면3


개시
유한 아핀 기하부호 선택
S21
열의 가중치의 최대값/부호화율 결정
S22
열과 행의 가중치 배분 계산(잠정)
S23
행의 가중치 선택/분할 계수 결정
S24
행의 가중치 비율 결정
S25
열의 가중치 배분 계산(잠정)
S26
열의 가중치의 후보 선택
S27
열과 행의 가중치 배분 계산
S28
가중치 배분 조정
S29
분할
S30

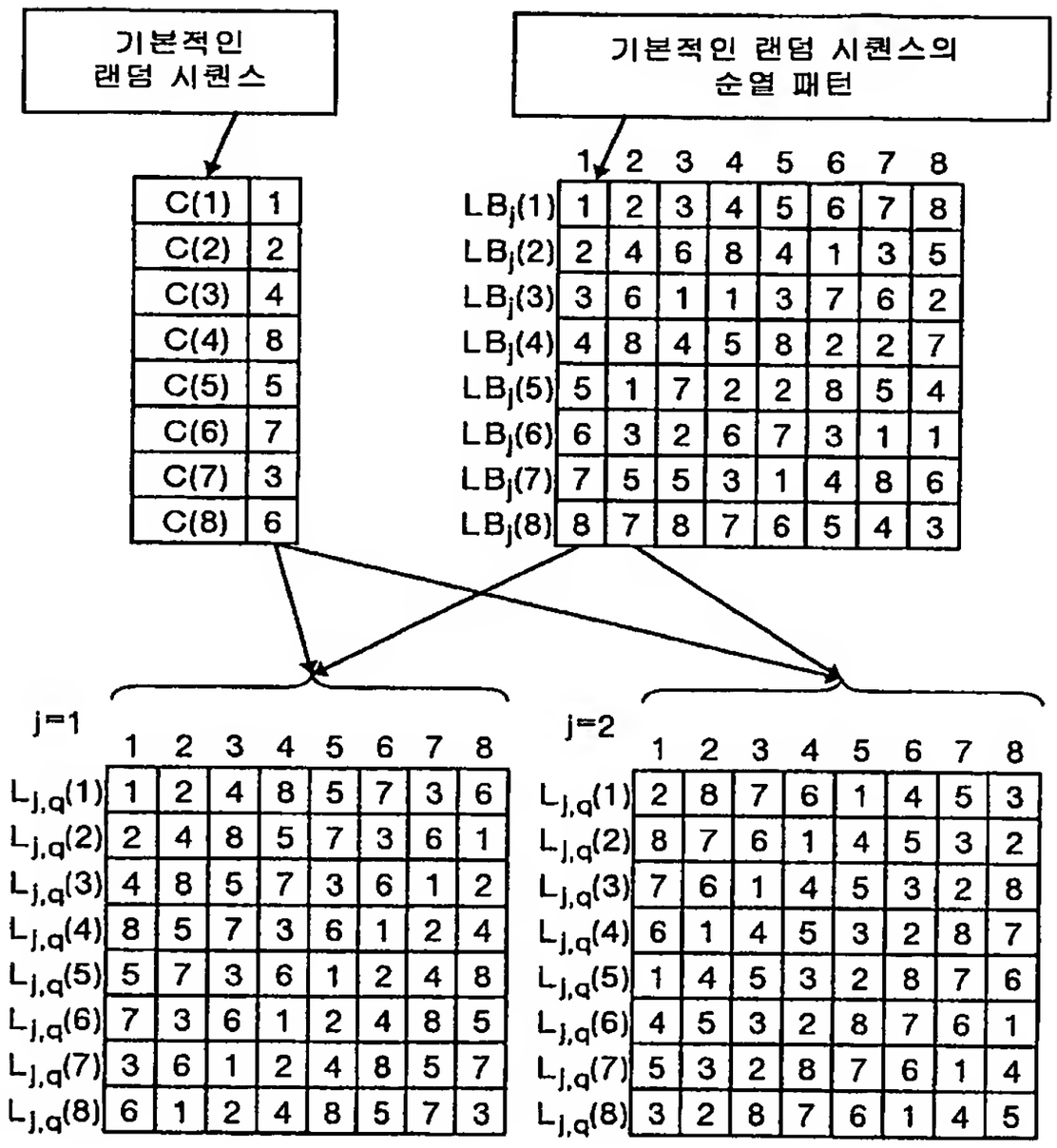
도면4



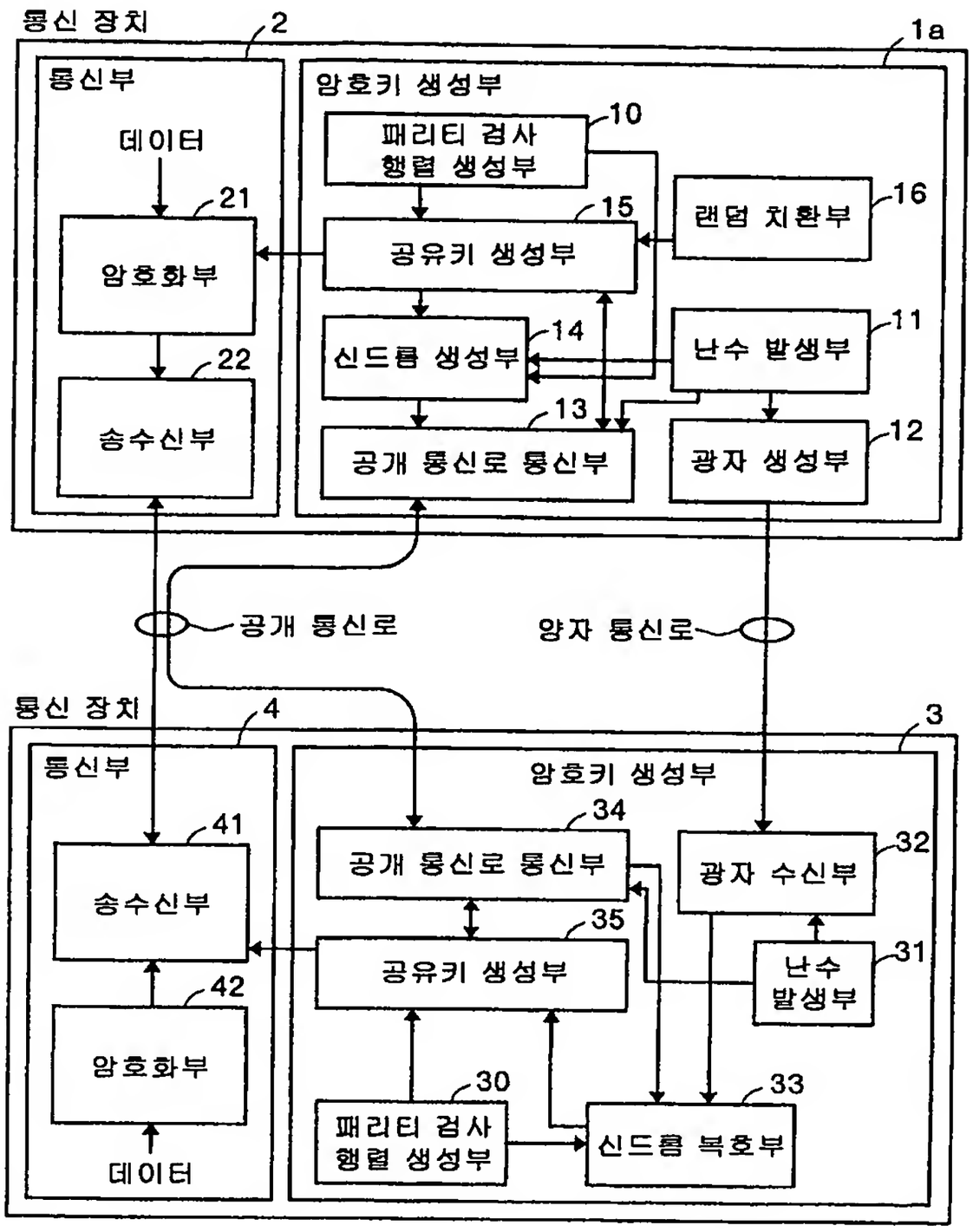
도면5

레이트		0.5	
N		12.6	
i	γ_i	$\lambda(\gamma_i)$	$n(\gamma_i)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
u		ρ_u	nu
8		1	63

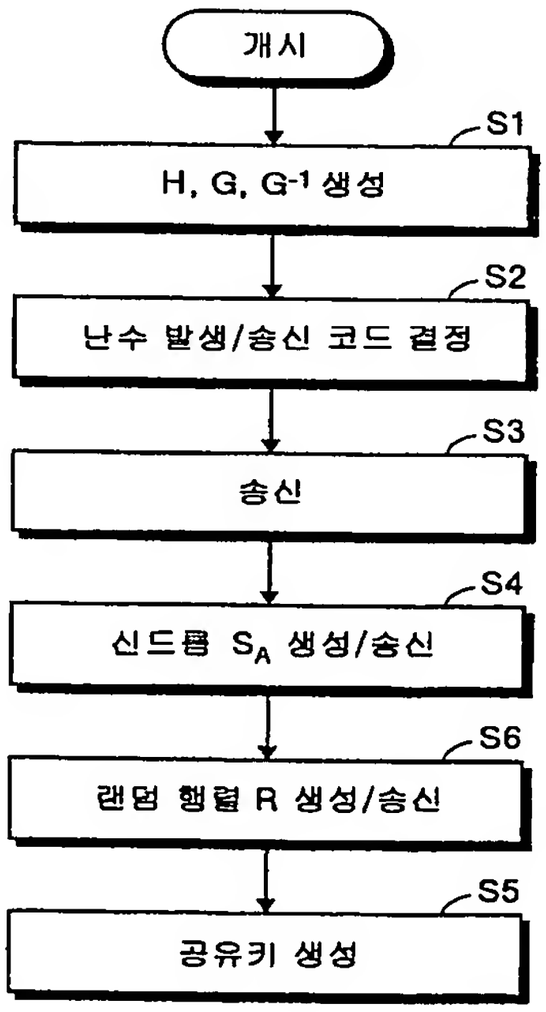
도면6



도면7


통신 장치
2
1a
통신부
데이터
21
암호화부
22
송수신부
암호키 생성부
10
패리티 검사
행렬 생성부
15
공유키 생성부
16
랜덤 치환부
14
신드롬 생성부
11
난수 발생부
13
공개 통신로 통신부
12
광자 생성부
공개 통신로
양자 통신로
통신 장치
4
3
통신부
암호키 생성부
41
송수신부
42
암호화부
데이터
34
공개 통신로 통신부
32
광자 수신부
35
공유키 생성부
31
난수
발생부
30
패리티 검사
행렬 생성부
33
신드롬 복호부

도면8


개시
S1
H, G, G-1 생성
S2
난수 발생/송신 코드 결정
S3
송신
S4
신드롬 SA 생성/송신
S6
랜덤 행렬 R 생성/송신
S5
공유키 생성

도면9